What Is Claimed Is:

1. A method for centralizing administration of user registration information across networks, characterized by: including at least an Internet Content Provider (ICP) and a user-login-identification means which can access an online terminal; wherein the ICP adds an interface module in a login web page and accesses the user-login-identification means via the interface module, and the ICP also provides an administration/drive module monitoring access of the user-login-identification means to set up a connection and hang up the connection for the user-login-identification means in the login web page; the user-login-identification means is provided with an ID number, and user's login identification information is stored in the user-login-identification means.

2. The method of claim 1, wherein ICP access authentication information is stored in the user-login-identification means to verify whether the accessing ICP is authorized to access; if the accessing ICP passed the verification, its access is permitted, otherwise the access is not permitted.

3. The method of claim 3 wherein the ICP is permitted to access the user-login-identification means only if it is authenticated, when the user-login-identification means is activated.

4. The method of claim 1, wherein the procedure of authenticating the ICP comprises, obtaining an authentication file via the interface module, transmitting the authentication file to the administration/drive module, decrypting the authentication file by the administration/drive module, and accessing the user-login-identification means.

5. The method of claim 4, wherein the authentication file includes ICP identification information and/or specific area guide information of the user-login-identification means and/or data processing guide information and/or time information.

6.The method of claim 1, wherein a registration table of the ICP identification information is stored in the user-login-identification means to guide

REPLACED BY
ART 34 AMDT

different ICPs to access only the corresponding areas or contents while accessing the user-login-identification means.

7. The method of claim 1, wherein different ICPs store and read respective login identification information in the corresponding areas of the user-login-identification means.

8. The method of claim 1, wherein the administration/drive module can also lead in and/or lead out data stored in the user-login-identification means so as to backup the data.

9. The method of claim 8, wherein the administration/drive module can also automatically log in, in the case that the ICP accesses the user-login-identification means via the interface module and verifies the identification information.

10. The method of claim 4, wherein the ICP accessing the user-login-identification means includes checking the user ID identification information stored in the user-login-identification means, or generating the user ID identification information in the user-login-identification means.

11. The method of claim 10, wherein the ICP reads the information stored in the user-login-identification means, and if login identification information is obtained, the interface module returns the login identification information to the ICP web page and determines whether a login-submit or an automatic submit & login should be performed according to user's setup; if the login identification information is not obtained, the interface module informs the web page that the login identification information is not available and stores the generated login identification information in the user-login-identification means.

12. The method of claim 11, wherein storing the login identification information includes the ICP storing the login identification information in the user-login-identification means via the interface module, in the case that the user logs in the ICP website for the first time, or the user selects to manually enter the login information once more, or the user-login-identification means is used for the first time.

13. The method of claim 10, wherein an ICP web page is provided with a registration information window; the ICP invokes parameters of the interface

module and simultaneously saves several sets of registration information of a same web page or saves the last set of registration information in the user-login-identification means, and the registration information can also be displayed on the ICP web page.

14. The method of claim 13, wherein the an ICP web page is provided with a registration information window; the ICP accesses the user-login-identification means via the interface module and verifies the login identification information provided by the ICP web page, and stores new login identification information in the user-login-identification means to overwrite original login identification information, and transfers relating information to the ICP web page; the information is displayed on the web page after being obtained.

15. The method of claim 13, wherein the ICP web page is provided with a plurality of window links of the registration information; the ICP reads the user-login-identification information stored in the user-login-identification means and verifies the login identification information provided by the ICP web page; if verification appears negative, the login identification information is stored in the user-login-identification means, and if positive, the login identification information is directly read out and the relating information is transferred to the ICP web page; the information is displayed on the web page after being obtained.

16. The method of claim , further includes a login verification serving party for implementing prior authentication to the ICP and obtaining guide information of the user-login-identification means.

17. The method of claim 16, wherein the ICP is connected with a login verification serving party which transmits a code for accessing the user-login-identification means to the ICP, and the ICP adds the login identification information in the login web page according to the code, and the interface module transmits the ICP information to the login verification serving party for verification; if the ICP information passed the verification, the ICP is permitted to access the user-login-identification means.

18. The method of claim 17, wherein the user activates the user-login-identification means by using a password, and then the ICP accesses the login verification serving party for an authentication via the interface module;

if the authentication is valid, the ICP can operate the user-login-identification means via the interface module.

19. The method of claim 18, wherein the actuating password used by the user is provided by the login verification serving party or preset in the means.

20. The method of claim 18, wherein the encryption files of the ICPs transmitted by the login verification serving party are different from each other.

21. The method of claim 16, wherein the login verification serving party maintains a database of authentication files so as to manage the authentication files.

22. The method o claim 21, wherein the login verification serving party is a server.

23. The method of any one of the above claims, wherein the user-login-identification information includes ICP identification information or form information or user identification information or combination of the above.

24.A system for realizing the method of any one of the above claims, characterized by, comprising a computer, Internet networks, an ICP and a user-login-identification means, wherein the computer can log in the Internet networks to communicate with different ICPs; the user-login-identification means is capable of accessing the computer from outside and has at least an identification number and encryption storage space; the user-login-identification means performs the information transmission by operating the computer.

25.The system of claim 24, wherein the ICP is connected with a login verification serving party which transmits a code for accessing the user-login-identification means to the ICP, and the ICP adds the login identification information in the login web page according to the code, and the interface module transmits the ICP information to the login verification serving party for verification; if the verification is valid, the ICP is permitted to access the user-login-identification means.

26. The system of claim 25, wherein the login verification serving party is a server.

27. The system of claim 24, wherein information transmission between the computer and the user-login-identification means should be processed with

REPLACED BY
ART 34 AMDT

encryption or decryption.

28. The system of claim 25, wherein the encryption includes protecting an encryption area by using the user's PIN code or utilizing RSA 512PKI key management encryption method.

29. The system of claim 24, wherein the user-login-identification means is also provided with a storage region for storing the information of the ICP itself.

30. The system of claim 29, wherein the user-login-identification means is an external and portable memory means with a standard data interface, or a card-reader means or an ID identifying means thereof .

31. The system of claim 30, wherein the user-login-identification means can be a USB storage device, a CF card, a MMC card, a SD card, a SMC card, an IBM Micro Drive card, a flash storage module or an IC card.

32. The system of claim 30, wherein the portable memory card-reader means can be a CF card processor, a MMC card processor, a SD card processor, a SMC card processor, an IBM Micro Drive card processor or an IC card processor.

33. The system of claim 29, wherein the user-login-identification means is a computer peripheral, such as a keyboard, a mouse, a handwriting board or sound boxes.

34. The system of claim 29, wherein the user-login-identification means is a portable PDA, a music player or an electrical dictionary.

REPLACED BY
ART 34 AMDT